UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FIME
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

Sistemas Operativos

Actividad Fundamental #4

Multitarea

Redes y Seguridad: Sistemas Distribuidos.

Docente: **Dra. Norma Edith Marín Martínez**

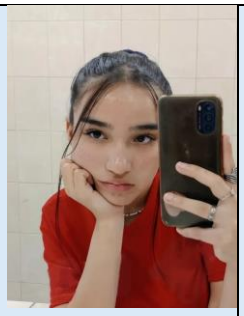
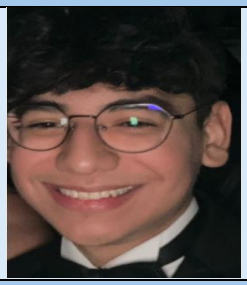
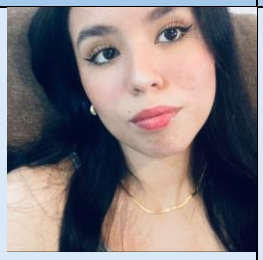
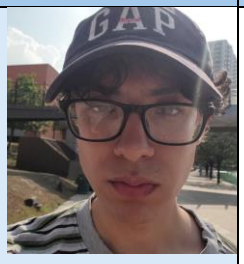
Hora: **M3** Salón: **9104**

Agosto – Diciembre 2024

Matrícula	Alumno	Carrera
1952809	Castillo Arreola Antonio	IAS
2041139	Álvarez García Angel Ricardo	ITS
2044753	Ramírez Núñez Brian Orlando	IAS
2049875	Sainz Coronado Alfonso	ITS
2051321	Garza Walle Alejandra	ITS
2055826	Salinas Monsiváis Emiliano	ITS
2109508	Martínez Tamez Valeria Guadalupe	IAS
2132048	Naranjo Rojas Horacio	ITS
2132062	Loredo Pérez Axel Arturo	ITS

Cd. Universitaria, San Nicolás de los Garza, N.L., a 3 de noviembre de 2024

Participantes en la Actividad Fundamental #3

					
Datos del alumno	**Horacio Naranjo Rojas 2132048 ITS**	**Brian Orlando Ramírez Nuñez 2044753 IAS**	**Ángel Ricardo Álvarez García 2041139 ITS**	**Alejandra Garza Walle 2051321 ITS**	**Antonio Castillo Arreola 1952809 IAS**
					
Datos del alumno	**Alfonso Sainz Coronado 2049875 ITS**	**Emiliano Salinas Monsiváis 2055826 ITS**	**Valeria Guadalupe Martínez Tamez 2109508 IAS**	**Axel Arturo Loredo Pérez 2132062 ITS**	

índice

Introducción

La **seguridad informática** busca proteger sistemas y datos de amenazas como el acceso no autorizado, el robo de información y los ataques que interrumpen servicios (DDoS). Los principales riesgos incluyen **virus** (software malicioso que se replica), **gusanos** (se propagan sin intervención humana), y otras formas de **malware** como troyanos (programas disfrazados), spyware (espía al usuario), adware (muestra anuncios) y ransomware (secuestra datos para pedir rescate).

Existen varios **tipos de intrusos**: externos (hackers) e internos (empleados con acceso autorizado). Para contrarrestarlos, se implementan **métodos de autenticación**, como contraseñas, autenticación multifactor (MFA) y biometría (huellas, reconocimiento facial).

Los **niveles de seguridad** varían según el entorno:

- **Usuario**: antivirus, contraseñas fuertes y MFA.
- **Red doméstica o pequeña oficina**: cortafuegos y VPN.
- **Empresa**: sistemas más avanzados como firewalls de red, IPS y auditorías regulares.

Que amenazas existen

A pesar de que las amenazas de seguridad son muy comunes hoy día y sus consecuencias pueden incluso acabar con una empresa en cuestión de horas, muchas de estas esperan a que ocurra algo para protegerse de las amenazas.

Ahora que la mayoría de nuestras actividades diarias están automatizados y disponibles en Internet, debemos ser más precavidos que cuando cruzamos la calle. Esta precaución es necesaria aún más después de ver surgir algunas estadísticas críticas, alegando que casi un tercio de las computadoras del mundo están infectadas con algún tipo de malware.

El delito cibernético ahora es un gran negocio y los delincuentes buscan robar información como detalles financieros, información de tarjetas de crédito, datos personales o cualquier otra información que puedan vender o intercambiar. Estos delincuentes son cada vez más sofisticados y emplean muchos métodos diferentes para atacar las redes informáticas de las empresas.

El uso de la Ingeniería social para explotar las debilidades humanas representa una amenaza de seguridad muy real y constante para todas las empresas. Es importante que estas reconozcan y tomen los pasos apropiados, para reducir la probabilidad de ser atacados y minimizar el impacto

Diferentes amenazas a la seguridad de la información

Malware

Malware es la abreviatura de «software malicioso». A la mayoría de las personas les viene a la mente fácilmente cuando piensan en amenazas a la seguridad de la información. El malware está diseñado para dañar o interrumpir los sistemas informáticos, robar datos u obtener acceso no autorizado.

El malware se presenta en muchas formas, como virus, gusanos, troyanos, software espía, secuestradores de navegador y programas publicitarios. El ransomware es un tipo de malware que cifra tus archivos y exige un pago a cambio de la clave de descifrado.

El malware puede ingresar a tu sistema a través de archivos adjuntos de correo electrónico, sitios web infectados o redes para compartir archivos. Puede robar tus datos personales, destruir tus archivos o utilizar tu computadora para atacar otros sistemas.

Ataques de Denegación de Servicio

Un ataque de denegación de servicio (DoS) es un tipo de ataque en el que un atacante inunda un sitio web o red con tráfico, lo que provoca que dejen de estar disponibles para usuarios legítimos. Los atacantes suelen lanzar ataques DDoS (denegación de servicio distribuido) mediante botnets, que consisten en redes de ordenadores comprometidos controlados remotamente.

Los atacantes suelen utilizar ataques DDoS para extorsionar a los propietarios de sitios web o interrumpir los servicios. A veces también utilizan estos ataques como táctica de distracción para distraer a los equipos de seguridad mientras se producen otros ataques.

Un ejemplo de un ataque DDoS es el ataque de 2016 a Dyn, un proveedor de sistema de nombres de dominio que utiliza un sistema de malware y botnet denominado Mirai. El ataque provocó una interrupción generalizada en sitios web y servicios, incluidos Twitter, Netflix y Amazon.

Ingeniería Social

La ingeniería social es un tipo de amenaza a la seguridad de la información que se basa en la manipulación del comportamiento humano en lugar de explotar vulnerabilidades técnicas. En otras palabras, en lugar de depender de errores de software u otras debilidades técnicas para obtener acceso a información o sistemas sensibles, los ingenieros sociales utilizan trucos psicológicos y engaños para convencer a las personas de que les den lo que quieren.

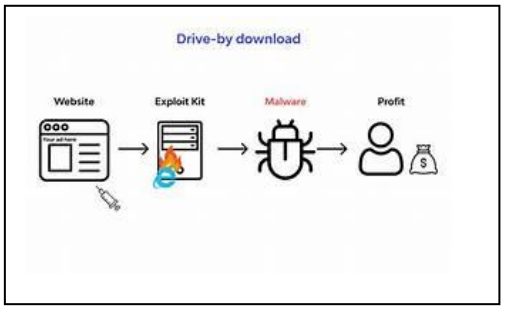
Los ataques de ingeniería social adoptan muchas formas diferentes, pero todos comparten el objetivo común de engañar a las personas para que divulguen información confidencial o concedan acceso a sistemas restringidos. La ingeniería social podría ocurrir de varias maneras. Uno de ellos es el pretexto, en el que los atacantes crean un pretexto falso para obtener acceso a información o sistemas confidenciales.

También podría implicar ataques de cebo que implican ofrecer algo de valor a cambio de información confidencial o acceso. Por ejemplo, un atacante podría dejar una unidad USB tirada en las instalaciones de una organización objetivo, etiquetada con una etiqueta tentadora como «Información de nómina de los empleados».

Ataques drive-by

Los ataques drive-by son un tipo de ciberataque que normalmente ocurre cuando un usuario visita un sitio web comprometido o hace clic en un enlace malicioso. El ataque se llama así porque ocurre “de paso”, sin el conocimiento ni la participación del usuario.

Los ataques no autorizados pueden ocurrir de varias maneras, pero los tipos más comunes implican la explotación de vulnerabilidades en el navegador web o los complementos de un usuario, como versiones obsoletas de Microsoft Office o extensiones del navegador.



Una vez que un usuario visita un sitio web comprometido o hace clic en un enlace malicioso, el código del atacante se ejecuta en la computadora del usuario, a menudo sin ninguna indicación visible para el usuario. Los ataques desde vehículos pueden tener graves consecuencias.

Los atacantes pueden utilizar ataques drive-by como una forma de afianzarse en un sistema o red, que luego pueden utilizar para llevar a cabo más ataques. Para protegerte contra ataques encubiertos, es importante mantener navegadores web y complementos actualizados.

Los usuarios también deben tener cuidado al visitar sitios web desconocidos o hacer clic en enlaces y deben tener cuidado con ventanas emergentes inesperadas o solicitudes para descargar software. Un programa antivirus de buena reputación también puede ayudar a detectar y prevenir ataques encubiertos bloqueando el código malicioso antes de que se ejecute.

Amenazas Internas

Una amenaza interna es un riesgo de seguridad que plantean los empleados u otras personas internas que tienen acceso a información confidencial. Las amenazas internas pueden ser intencionadas, como cuando un empleado roba datos para beneficio personal o para venderlos en el mercado negro. También pueden ser involuntarias, como cuando un empleado elimina o comparte accidentalmente datos confidenciales.

Las amenazas internas suelen ser difíciles de detectar ya que los atacantes tienen acceso legítimo al sistema. Sus aplicaciones incluyen el robo de datos, el beneficio económico o el sabotaje. Un ejemplo de amenaza interna es el caso de Edward Snowden, en el que un excontratista de la Agencia de Seguridad Nacional (NSA) filtró información clasificada a los medios de comunicación.

Puedes prevenir amenazas internas implementando estrictos controles de acceso y monitoreando la actividad de los empleados. Capacitar a los empleados sobre las mejores prácticas de seguridad también puede reducir el riesgo de amenazas internas no intencionales.

Ataque Man in the Middle

Los ataques Man in the Middle (MitM) ocurren cuando un atacante intercepta las comunicaciones entre dos partes. El atacante puede entonces escuchar la conversación, modificar la comunicación o hacerse pasar por una de las partes. Los atacantes pueden lograr esto explotando las vulnerabilidades de la red o utilizando técnicas de ingeniería social para engañar a los usuarios para que se conecten a una red falsa.

Los atacantes suelen utilizar ataques MitM para robar información confidencial, como credenciales de inicio de sesión o datos financieros, así como

para lanzar más ataques o interrumpir servicios. MitM podría tomar la forma del ataque SSLstrip, donde un atacante intercepta las comunicaciones entre un usuario y un sitio web, degradando la conexión a una no cifrada usando HTTP en lugar de HTTPS.

El grupo de hackers Darkhotel utilizó popularmente ataques MitM para robar información confidencial de objetivos de alto perfil, incluidos funcionarios gubernamentales y ejecutivos de la industria hotelera.

Puedes prevenir ataques MitM usando cifrado y firmas digitales, usando conexiones seguras y evitando la Wi-Fi pública.

Inyección SQL

La inyección SQL implica insertar código malicioso en la base de datos de un sitio web para obtener acceso no autorizado o robar información. Los atacantes pueden lograr la inyección SQL explotando las vulnerabilidades en el código del sitio web o engañando a los usuarios para que ejecuten código SQL malicioso utilizando técnicas de ingeniería social.

Los ataques de inyección SQL permiten a los atacantes robar información confidencial, modificar o eliminar datos u obtener acceso no autorizado. Un ejemplo popular de un ataque de inyección SQL es la violación de datos de Equifax de 2017, donde los atacantes explotaron una vulnerabilidad de inyección SQL para obtener acceso a datos confidenciales como números de seguro social y fechas de nacimiento.

Tipos de Virus

Los virus informáticos son programas maliciosos diseñados para alterar el funcionamiento normal de un sistema informático. Estos programas pueden replicarse y propagarse a otros sistemas, causando desde pequeños inconvenientes hasta pérdidas económicas significativas.

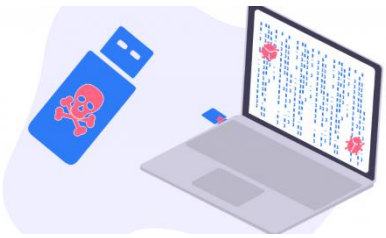
Tipos de Virus Informáticos y sus Funciones

A continuación, exploraremos con mayor detalle algunos de los tipos de virus informáticos más comunes y sus características:

Virus de Archivo:

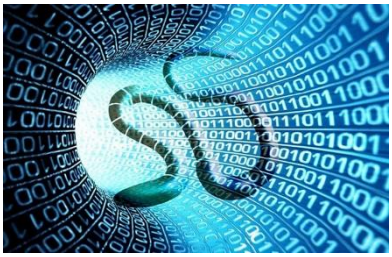
- Infectan archivos ejecutables, documentos y otros tipos de archivos.
- Pueden alterar el contenido de los archivos, hacerlos inutilizables o incluso ejecutar código malicioso cuando se abre el archivo.
- **Ejemplo:** Un virus que infecta un documento de Word y agrega código malicioso que se ejecuta cuando se abre el documento.
-

Virus de Boot:



- Infectan el sector de arranque del disco duro, el cual contiene las instrucciones necesarias para iniciar el sistema operativo.
- Se ejecutan cada vez que se enciende el equipo, lo que dificulta su eliminación.
- **Ejemplo:** Un virus que modifica el sector de arranque para que en lugar de iniciar el sistema operativo, se ejecute un programa malicioso.

Gusanos:



- Se propagan automáticamente a través de redes, sin necesidad de la intervención del usuario.
- Pueden consumir grandes cantidades de ancho de banda y recursos del sistema.
- **Ejemplo:** El gusano Morris, uno de los primeros gusanos conocidos, explotó una vulnerabilidad en el sistema operativo Unix para propagarse rápidamente por Internet.

Troyanos:

- Se disfrazan de programas legítimos para engañar a los usuarios y obtener acceso a sus sistemas.
- Una vez dentro, pueden realizar diversas acciones maliciosas, como robar información, abrir puertas traseras o descargar otros tipos de malware.
- **Ejemplo:** Un troyano que se hace pasar por un reproductor de música y, una vez instalado, roba las contraseñas almacenadas en el navegador.

Rootkits:

- Ocultan su presencia en el sistema operativo, dificultando su detección y eliminación.
- Pueden modificar el kernel del sistema operativo, lo que les permite controlar prácticamente todos los aspectos del sistema.
- **Ejemplo:** Un rootkit que oculta las actividades de un troyano bancario, permitiendo al atacante robar dinero de las cuentas bancarias del usuario.

Ransomware:

- Cifran los archivos del usuario y exigen un pago a cambio de la clave de descifrado.
- Pueden cifrar tanto archivos individuales como discos duros completos.
- **Ejemplo:** Un ransomware que cifra todos los archivos de un usuario y muestra un mensaje en pantalla exigiendo el pago de un rescate en criptomonedas.

Vectores de Ataque y Métodos de Propagación

Los virus se propagan a través de diversos métodos, entre los que se incluyen:

- **Correo electrónico:** Adjuntos infectados, enlaces a sitios web maliciosos o phishing.
- **Descargas de Internet:** Archivos infectados descargados de sitios web no confiables o redes P2P.
- **Dispositivos de almacenamiento:** Memorias USB, discos duros externos infectados.
- **Explotación de vulnerabilidades:** Los atacantes buscan y explotan vulnerabilidades en software y sistemas operativos para infectar equipos.

Cómo Protegerse de los Virus Informáticos

- **Mantén tu sistema actualizado:** Instala las últimas actualizaciones de seguridad para tu sistema operativo y software.
- **Utiliza un antivirus de confianza:** Un buen antivirus puede detectar y eliminar virus en tiempo real.

- **Sé cauteloso con los correos electrónicos y enlaces:** No abras archivos adjuntos ni hagas clic en enlaces de remitentes desconocidos.
- **Descarga software solo de fuentes confiables:** Evita descargar software de sitios web sospechosos.
- **Realiza copias de seguridad regularmente:** Las copias de seguridad te permiten restaurar tus archivos en caso de infección.
- **Educa a los usuarios:** La concientización sobre las amenazas cibernéticas es fundamental para prevenir infecciones.

Los virus informáticos representan una amenaza constante para la seguridad de nuestros sistemas y datos. Al comprender los diferentes tipos de virus y siguiendo las mejores prácticas de seguridad, podemos proteger nuestros equipos y minimizar el riesgo de infección.

Gusanos Malware: troyano, spyware, adware, ransomware.

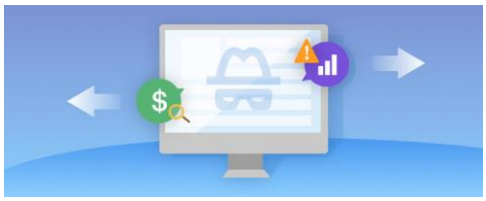
Troyano.

Los Troyanos (o "Trojan Horses") es un término referido a un tipo de software malicioso que se "disfraza" para ocultar sus verdaderas intenciones. Sin embargo, a diferencia de los virus, no puede expandirse ni infectar archivos por sí solo. Para infiltrarse en el dispositivo de una víctima, esta categoría de malware se basa en otros medios, como descargas automáticas, explotación de vulnerabilidades, descarga por otro código malicioso o técnicas de ingeniería social.

Los troyanos son actualmente la categoría de malware más común, y son utilizados habitualmente para abrir backends, tomar el control del dispositivo afectado, filtrar los datos del usuario y enviarlos a terceros, descargar y ejecutar otro software malicioso en el sistema, así como para muchos otros objetivos nefastos para el usuario.

Spyware

Es un programa de software que puede registrar de manera secreta su actividad en una computadora. Comúnmente, llega mediante una descarga gratuita o un documento adjunto infectado en un correo electrónico. Esto se conoce como caballo de Troya. Basta un clic para instalar un spyware en su computadora sin su conocimiento. Después de instalarse, el spyware se oculta en el sistema operativo y no lo puede ver.



Eso dificulta la detección del spyware, y es incluso más difícil de desinstalar. Mientras el spyware se ejecuta en segundo plano, usted está en riesgo de exponer información confidencial, como hábitos de navegación en Internet, contraseñas, direcciones de correo electrónico y otros datos.

Adware

El adware es un programa que muestra anuncios emergentes no deseados (y a veces irritantes) que pueden aparecer en tu computadora o dispositivo móvil. El adware suele llegar a los dispositivos de los usuarios por dos vías:

1. Es posible que instales un programa informático o una aplicación gratuita sin darte cuenta de que contiene adware adicional. Esto le permite al desarrollador de la aplicación ganar dinero, pero significa que podrías descargar adware en tus sistemas sin dar tu consentimiento.
2. Otra posibilidad es que exista una vulnerabilidad en el software o en el sistema operativo que los hackers aprovechen para introducir malware, incluidos algunos tipos de adware, en el sistema.

El adware se instala de forma silenciosa en los dispositivos del usuario con la esperanza de que haga clic en los anuncios que muestra, por accidente o no.

Esto se debe a que, en última instancia, el adware existe para ganar dinero.

Los creadores de adware y los vendedores que lo distribuyen obtienen dinero de terceros a través de lo siguiente:

1. Pago por clic (PPC): cobran cada vez que abres un anuncio.
2. Pago por visión (PPV): cobran cada vez que se te muestra un anuncio.
3. Pago por instalación (PPI): cobran cada vez que se instala un paquete de software en un dispositivo.

El adware también puede rastrear tu historial de búsqueda y navegación para mostrarte anuncios más relevantes para ti. Una vez que el desarrollador tiene tu ubicación e historial de navegación, puede obtener ingresos adicionales vendiéndole esa información a terceros.

Ransomware

El ransomware es un tipo de malware que retiene los datos o el dispositivo confidenciales de una víctima, amenazando con mantenerlos bloqueados, o peor, a menos que la víctima pague un rescate al atacante.

El ransomware es un tipo de malware diseñado para extorsionar dinero a sus víctimas, quienes están bloqueadas o impedidas de acceder a los datos en sus sistemas. Los dos tipos más frecuentes son los cifradores y los bloqueadores de pantalla. Los cifradores, como su nombre sugiere, cifran los datos en un sistema para que el contenido quede inutilizado si no se tiene la clave de descifrado. Los bloqueadores de pantallas, por otra parte, simplemente bloquean el acceso al sistema con una pantalla de “bloqueo”, afirmando que el sistema está cifrado.

Las víctimas suelen ser notificadas en una pantalla de bloqueo (muy común tanto en los cifradores como en los bloqueadores de pantalla) de que deben comprar una criptomoneda, como el Bitcoin, para pagar el rescate. Una vez pagado el rescate, los clientes reciben la clave de descifrado y pueden intentar descifrar los archivos. El descifrado no está garantizado, y hay múltiples fuentes que reportan

diferentes niveles de éxito con el descifrado después de pagar los rescates. A veces las víctimas simplemente no llegan a recibir las claves. Algunos ataques instalan el malware en el sistema informático incluso después de haberse pagado el rescate y liberados los datos.

Autenticación

La autenticación es el proceso utilizado para confirmar que solo las personas, servicios y aplicaciones adecuados con los permisos correctos pueden acceder a diferentes recursos del sistema. Es una parte importante de la ciberseguridad porque la mayor prioridad de un infiltrado es obtener acceso no autorizado a los sistemas. Para llevar esto a cabo, roban el nombre de usuario y las contraseñas de los usuarios que sí tienen acceso. El proceso de autenticación incluye tres pasos principales:

- **Identificación**: Los usuarios establecen quiénes son a través de un nombre de usuario, normalmente.
- **Autenticación**: Normalmente, los usuarios prueban que son quienes dicen ser al escribir una contraseña (algo que, supuestamente, solo conoce el propio usuario); sin embargo, para

fortalecer la seguridad, muchas organizaciones también solicitan que prueben su identidad mediante algo que poseen (un teléfono o dispositivo de tokens) o algo que son (una huella dactilar o escáner facial).

- **Autorización**: El sistema comprueba que los usuarios tengan permisos para el sistema al que intentan acceder.

Tipos de autenticaciones

En la autenticación moderna, el proceso se delega en un sistema de identidad independiente de confianza, al contrario que en la autenticación tradicional, en la que cada sistema verifica identidades por sí mismo. También ha habido un cambio en el tipo de métodos de autenticación que se usan. La mayoría de las aplicaciones requieren un nombre de usuario y contraseña. Los infiltrados utilizan cada vez métodos más inteligentes para el robo de contraseñas, por lo que la comunidad de seguridad ha desarrollado varios métodos nuevos para ayudar a proteger las identidades.

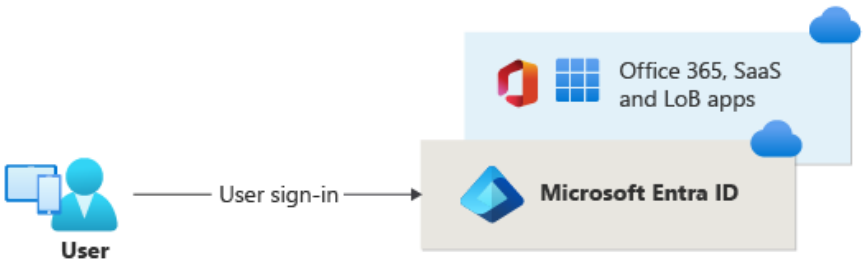
Autenticación basada en contraseña

La autenticación basada en contraseña es la forma de autenticación más frecuente. Muchas aplicaciones y servicios requieren que las personas creen contraseñas formadas por una combinación de números, letras y símbolos para reducir el riesgo de que un infiltrado las adivine. Sin embargo, las contraseñas también crean desafíos respecto a la seguridad y el uso. A las personas les resulta difícil crear y memorizar una contraseña exclusiva para cada una de sus cuentas online, razón por la que suelen reutilizar contraseñas. Además, los atacantes utilizan muchas tácticas para adivinar o robar contraseñas, o para engañar a las personas para que las compartan involuntariamente. Por esta razón, las

organizaciones han ido buscando otros métodos de autenticación más seguros en detrimento de las contraseñas.

Autenticación basada en certificado

La autenticación basada en certificado es un método cifrado que permite que los dispositivos y las personas se identifiquen en otros dispositivos y sistemas. Dos ejemplos frecuentes son las tarjetas inteligentes y el envío de certificados digitales a una red o servidor por parte del dispositivo de un empleado.

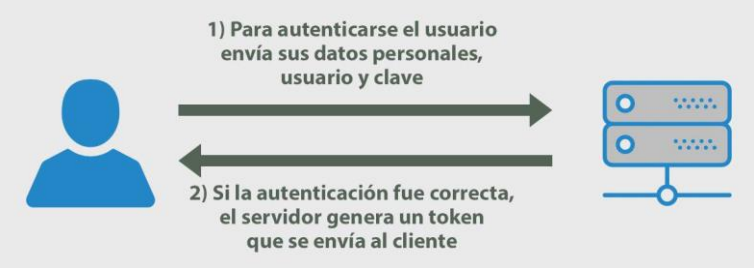


Autenticación biométrica

La autenticación biométrica se basa en la verificación de la identidad de una persona mediante sus características biológicas. Por ejemplo, muchas personas utilizan un dedo para iniciar sesión en sus teléfonos, y algunos ordenadores escanean la cara o la retina de una persona para verificar su identidad. Además, los datos biométricos se vinculan a un dispositivo específico, lo que hace que los atacantes no puedan usarlos sin obtener también acceso al dispositivo. Este tipo de autenticación es cada vez más popular debido a su facilidad de uso para las personas (ya que no necesitan memorizar nada) y a su dificultad de robo para los infiltrados, lo que lo hace más seguro que las contraseñas.

Autenticación basada en tokens

En la autenticación basada en tokens, tanto el dispositivo como el sistema generan un nuevo número singular llamado PIN temporal de un solo uso (TOTP) cada 30 segundos. Si los números coinciden, el sistema comprueba que el usuario tiene el dispositivo.



Contraseña de un solo uso

Las contraseñas de un solo uso (OTP) son códigos generados para un evento de inicio de sesión específico que expiran al poco de expedirse. Se entregan mediante mensaje SMS, correo electrónico o un token de hardware.

Notificación push

Algunas aplicaciones y servicios usan notificaciones push para autenticar a los usuarios. En estos casos, las personas reciben un mensaje en su teléfono que les solicita la aprobación o denegación del acceso solicitado. Debido a que las personas en ocasiones aprueban notificaciones push accidentalmente aunque estén intentando iniciar sesión en el servicio que envió la notificación, este método a veces se combina con un método de OTP. Con OTP, el sistema genera un número singular que el usuario tiene que escribir. Esto hace que la autenticación sea más resistente al phishing.

Autenticación por voz

En la autenticación por voz, la persona que intenta acceder a un servicio recibe una llamada telefónica en la que se les solicita introducir un código o identificarse de forma verbal.

Autenticación multifactor

Una de las mejores formas de reducir el riesgo de vulneración de cuentas es requerir dos o más métodos de autenticación, entre los que se pueden incluir cualquiera de los enumerados anteriormente. Un procedimiento recomendado eficaz es requerir dos de los siguientes métodos:

- Algo que el usuario conozca, normalmente una contraseña.
- Algo que el usuario posea, como un dispositivo de confianza que no se pueda duplicar fácilmente; por ejemplo, un teléfono o token de hardware.
- Algo que el usuario sea, como una huella dactilar o escáner facial.

Por ejemplo, muchas organizaciones solicitan una contraseña (algo que el usuario conoce) y también envían una OTP a través de SMS a un dispositivo de confianza (algo que el usuario posee) antes de permitir el acceso.

Autenticación con dos factores

La autenticación con dos factores es un tipo de autenticación multifactor que requiere dos formas de autenticación.

Niveles de Seguridad: Usuario, Redes y Empresas

En un mundo cada vez más digitalizado, la seguridad informática es una prioridad para individuos, redes y empresas. Proteger la integridad, confidencialidad y disponibilidad d e la información es crucial para evitar pérdidas económicas, daños a la reputación y otr os riesgos asociados con la ciberseguridad.

Seguridad para Usuarios Individuales

Los usuarios individuales son la primera línea de defensa en la seguridad informática.

Medidas esenciales incluyen:

1. **Antivirus y Antimalware**: El uso de programas de antivirus y antimalware actual izados protege contra una amplia variedad de amenazas, desde virus hasta rans omware.

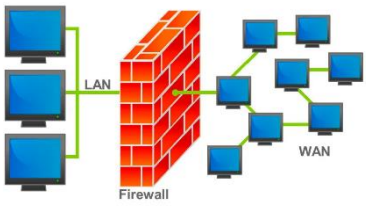
2. **Contraseñas Seguras y Autenticación Multifactor**: Contraseñas robustas com binadas con la autenticación de dos factores (2FA) o multifactor (MFA) añaden u na capa extra de seguridad.
3. **Cifrado de Datos**: El cifrado asegura que la información sensible esté protegida contra accesos no autorizados.

4. **Actualizaciones Regulares**: Mantener el sistema operativo y las aplicaciones a ctualizadas ayuda a cerrar vulnerabilidades conocidas.

Seguridad en Redes

Las redes, tanto domésticas como empresariales, requieren medidas específicas para protegerse contra intrusiones y ataques.

1. **Firewalls**: Los firewalls actúan como una barrera entre una red interna segura y



   redes externas no confiables, filtrando el tráfico malicioso.

2. **Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)**: Estos sistema s monitorizan el tráfico de red para detectar y prevenir actividades sospechosas.

3. **VPNs (Redes Privadas Virtuales)**: Las VPNs aseguran las conexiones remotas

   , protegiendo la privacidad y los datos que se transmiten.

4. **Segmentación de Red**: Dividir una red en segmentos ayuda a limitar la propaga ción de ataques y a proteger áreas críticas.

Seguridad en Empresas

Las empresas enfrentan desafíos de seguridad más complejos debido al volumen y sen sibilidad de los datos que manejan.

1. **Políticas de Seguridad**: Establecer políticas claras y comprensibles que todos l os empleados deben seguir es esencial.

2. **Capacitación en Seguridad**: Formar a los empleados sobre prácticas seguras y la identificación de amenazas ayuda a mitigar riesgos internos.

3. **Seguridad en la Nube**: Proteger datos y aplicaciones en la nube mediante cifrad o y gestión de identidades es fundamental.
4. **Auditorías y Evaluaciones de Riesgo**: Las auditorías periódicas y las evaluaci ones de riesgo identifican vulnerabilidades y ayudan a implementar mejoras cont inuas.
5. **Gestión de Incidentes**: Tener un plan de respuesta a incidentes permite a las e mpresas reaccionar rápidamente ante brechas de seguridad.
6. **Autenticación Multifactor (MFA)**: Utilizar múltiples métodos de autenticación as egura el acceso a sistemas críticos, reduciendo el riesgo de accesos no autoriza dos.

Conclusión Grupal

Para finalizar con el trabajo, tenemos que los diferentes temas que se abarcaron en este trabajo fueron de suma importancia sobre todo para el como manejamos los dispositivos, ya que con esto generamos conciencia de donde proteger la información y como optimizar los recursos. Este trabajo ha resaltado para entender las diversas amenazas que hay dentro del mundo informático, como los programas malignos, ataques internos, ingeniería social, y el como los podemos evitar con base a la autenticación de dos pasos, el uso de un buen antivirus, etc.

Se sabe que en conjunto las estrategias de ciberseguridad permiten que, al momento de crear un entorno informático seguro, genera confianza entre nosotros como usuarios, así como en el ámbito empresarial, sin anda más que añadir, damos por terminado el trabajo.

Conclusiones Individuales

Horacio Naranjo Rojas 2132048

La seguridad informática requiere un enfoque integral y multidimensional que abarca desde medidas básicas para usuarios individuales hasta complejas estrategias empresariales. Implementar niveles adecuados de seguridad según el contexto y la escala es clave para proteger la información en el entorno digital actual.

Antonio Castillo Arreola 1952809

Para concluir, es importante tener conocimiento acerca de cada uno de los virus o peligros que podemos tener en nuestros sistemas operativos. Hoy en día, es muy común ver ataques o amenazas en contra del usuario, por lo cual es importante tener un enfoque de seguridad ante cada una de ellas. Podemos correr riesgos y peligros al tener nuestra información a simple vista. Por último, sabemos que cada gusano malware tiene diferentes finalidades y es importante contar con alguna seguridad y prevención para cada una de ellas.

Alfonso Sainz Coronado 2049875 ITS

En mi conclusión, considero que el uso de gestores de paquetes como APT y DNF refleja tanto la fortaleza como la complejidad del ecosistema Linux. Aunque al principio pueden resultar complicados para usuarios acostumbrados al software de Windows, se dan cuenta de el gran potencial que tienen estas herramientas. Me parece muy util cómo estos gestores no solo automatizan la instalación de software, sino también la gestión de dependencias, lo que evita muchos problemas. Además, la capacidad de actualizar todo el sistema desde la terminal con un solo comando es algo que beneficia de gran manera ya que optimiza el mantenimiento del sistema.

Valeria Guadalupe Martínez Tamez 2109508 IAS

En conclusión, se podría decir que deberíamos estar bien informados acerca de las amenazas que existen hacia nuestros equipos, como de las que se hablaron en esta actividad, los malware, amenazas internas, ataques drive-by, etc. Para saber qué hacer si nos pasa o también para tomar algún tipo de medidas para que no nos llegue a afectar.

Ángel Ricardo Álvarez García 2041139 ITS

La seguridad es de suma importancia, sobre todo en los dispositivos de software, ya que en estos nosotros guardamos diferente tipo de información de suma relevancia, yendo desde cuentas de banco, fotos personales, etc. Vimos las diferentes tipos de amenazas que se

pueden provocar dentro de este ámbito y el cómo se pueden identificar.Finalizando con lo que se pueden implementar en nivel de seguridad como usuario y el nos beneficia.

Emiliano Salinas Monsiváis 2055826 ITS

Para finalizar con esta investigación, la seguridad en el software es esencial para proteger los datos y sistemas de amenazas como virus, malware y ataques cibernéticos. Implementar contraseñas robustas, mantener el software actualizado y usar herramientas de seguridad confiables son medidas clave para prevenir ataques. Además, es importante realizar copias de seguridad y capacitar a los usuarios sobre las amenazas más comunes. Mantenerse informado es crucial, ya que las amenazas evolucionan constantemente y estar preparado reduce riesgos y protege tanto los sistemas como la información.

Axel Arturo Loredo Pérez 2132062 ITS

Es esencial estar informados sobre los distintos tipos de virus y amenazas que pueden afectar nuestros sistemas operativos, ya que los ataques contra los usuarios son cada vez más comunes. La seguridad debe ser una prioridad para proteger nuestra información. Además es importante reconocer que el uso de herramientas como los gestores de paquetes, además de simplificar la instalación y actualización de software, contribuye al buen mantenimiento del sistema y facilita la gestión de las dependencias, ayudando a prevenir posibles problemas.

Brian Orlando Ramírez Nuñez 2044753 IAS

En el entorno empresarial, es fundamental adoptar estrategias más complejas y específicas. Estas incluyen la implementación de políticas de seguridad rigurosas, como la segmentación de redes, el uso de sistemas de gestión de vulnerabilidades y la capacitación continua del personal. También es clave emplear herramientas avanzadas, como gestores de paquetes en sistemas Linux para mantener actualizaciones centralizadas y seguras, garantizando la protección de datos sensibles y minimizando interrupciones operativas.

Alejandra Garza Walle 2051321 ITS

La seguridad digital comienza con pasos simples que cualquier usuario puede implementar. Entre las medidas básicas están: la creación de contraseñas robustas, la actualización periódica del software y el uso de herramientas de seguridad confiables, como antivirus. Estas acciones minimizan el riesgo de ataques, protegiendo tanto la información personal como la estabilidad del sistema. A su vez, estar informado sobre las amenazas comunes, como malware o ataques drive-by, permite una mejor prevención y reacción ante posibles riesgos

Bibliografías

Aguilera, A. (s. f.). 10 tipos diferentes de amenazas a la seguridad de la información. Tecno Simple. https://tecno-simple.com/10-tipos-diferentes-de-amenazas-a-la-seguridad-de-la-informacion/#Ingenieria_Social

Redacción 2023 GAU. (2023, 26 julio). ¿Cómo proteger a tu celular de un virus o un malware? | .: Paréntesis :. https://parentesis.com/noticias/smartphones/Como_proteger_a_tu_celular_de_un_virus_o_un_malware

¿Qué es un malware de tipo «Troyano»? Cómo eliminarlo y permanecer protegido | ESET. (s. f.). ESET. https://www.eset.com/es/caracteristicas/malware-troyano/

Juniper Networks. (s. f.). ¿Qué es un spyware? | Juniper Networks. https://www.juniper.net/mx/es/research-topics/what-is-spyware.html

¿Qué es el adware? (2017, 16 noviembre). /. https://latam.kaspersky.com/resource-center/threats/adware

Ransomware – Qué es y cómo protegerse | Proofpoint ES. (2023, 1 diciembre). Proofpoint. https://www.proofpoint.com/es/threat-reference/ransomware

Szell, C. (2024, February 2). Intrusos informáticos: Hackers y Crackers - Conecta Magazine. Conecta Magazine. https://www.conectasoftware.com/magazine/hackers-crackers-no-galletas-definiendo-tipos-intrusos/

Bello, E. (2023, November 8). Ciberseguridad: Tipos de ataques y en qué consisten. Thinking for Innovation. https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Borrelli, M. (2013). Malware and Computer Security Incidents: Handling Guides. Nova S cience Publishers, Inc. ***https://cutt.ly/ag6lHtK***

Costas Santos, J. (2015). Seguridad informática. RA-MA Editorial. ***https://elibro.net/es/lc/unapec/titulos/62452***

Escrivá Gascó, G. (2013). Seguridad informática. Macmillan Iberia, S.A. ***https://elibro.net/es/lc/unapec/titulos/43260***

Rocha Haro, C. A. (2011). La Seguridad Informática. Revista Ciencia Unemi, 4(5), 26-33. ***https://www.redalyc.org/pdf/5826/582663867004.pdf***

¿Qué es la autenticación? Definición y métodos | Seguridad de Microsoft. (s. f.). https://www.microsoft.com/es-mx/security/business/security-101/what-is-authentication

Métodos de autenticación. (2021, 12 octubre). Viafirma. https://www.viafirma.com/es/metodos-de-autenticacion/